SUMMARY OF TESTIMONY OF BOB DYKES, CEO NEBUAD, INC.
BEFORE THE HOUSE SUBCOMMITTEE ON
TELECOMMUNICATIONS AND THE INTERNET
WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE:
DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES
July 17, 2008

My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with Internet Service Providers (ISPs). I come from a security background, serving for many years as Executive Vice President of Symantec Corporation. When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. As part of its mission, NebuAd sought to address these privacy and security concerns, ensuring it was in compliance with both the letter and spirit of the law. Appended to my testimony is a memorandum discussing in greater detail NebuAd's compliance with the law, including the cable privacy statute.

Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual web-sites to networks of web-sites. NebuAd system uses a select set of a user's Internet activities to construct anonymous inferences about likely interests, which are then used to select and serve the most relevant advertisements. In operating this service, NebuAd:

- Provides users with prior, robust notice and the opportunity to express informed choice about whether to participate, both before the service takes effect and persistently thereafter;
- Does not collect or use personally-identifiable information ("PII");
- Does not store raw data linked to identifiable individuals; and
- Provides state-of-the art security for any information stored.

As a result, NebuAd's service is designed so that no one – not even the government – can determine the identity of our users.

In the US, privacy statutes have been developed in a largely sector-specific fashion. This Subcommittee has long been part of that trend, having overseen the creation of privacy statutes covering the cable and telecommunications industries. Yet, even though these and other privacy statutes have been developed one at a time, there are common threads running through them:

- When more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed.
- When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business-neutrality.

TESTIMONY OF BOB DYKES, CEO NEBUAD, INC.
BEFORE THE HOUSE SUBCOMMITTEE ON
TELECOMMUNICATIONS AND THE INTERNET

WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE:
DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES
July 17, 2008

Chairman Markey, Ranking Member Stearns, and Members of the Subcommittee, thank you for inviting me to appear today to discuss the privacy implications of online advertising solutions in which Internet Service Providers (ISPs) participate. My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with ISPs. I have spent considerable time over the past year with federal policymakers at the Federal Trade Commission, Federal Communications Commission, and in Congress – as well as with consumer and privacy advocates – discussing NebuAd's technology, operations, and privacy protections and welcome the opportunity to discuss all of this further with the Subcommittee.

The NebuAd service in partnership with ISPs provides consumers with significant benefits, serving them with more relevant ads, which they want, while ensuring they have robust privacy protections and control over their online experience.

NebuAd's Ad Network also is designed to benefit two groups that provide substantial value on the Internet:

- The many smaller web sites and general news sites that have difficulty maintaining free access to their content;
- The ISPs who need to upgrade their infrastructure to provide increased bandwidth for consumers, who increasingly want access to Internet-delivered videos.

INTRODUCTION

Online advertising is a phenomenon of the Internet age. It permits advertisers to provide more relevant messages to consumers and in turn fuels the development of website publishers, both large and small. In fact, advertising is the engine for the free Internet. Within this world of online advertising, NebuAd and its ISP partners are newcomers, just entering among industry giants like Google, Yahoo!, Microsoft, Amazon, and countless website publishers. That means we have a steep hill to climb, but it also means we have great opportunities. We are able to learn the lessons of the industry and construct state-of-the-art technology that delivers ads that are more relevant to users and that provide them with robust and industry-leading privacy protections. Indeed, as I will discuss, these privacy protections are built into our technology and designed into our policies from the ground up.

Let me explain our privacy motivation more fully. I come from a security background, serving for many years as Executive Vice President of Symantec Corporation, a global leader in providing security solutions for computers and computer networks. When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. Hackers were piercing firewalls, seeking to capture seemingly random strands of data to find the identity of users. The government was ordering ISPs and other network providers to turn over data on their users. As part of its mission, NebuAd sought to address these privacy and security concerns, ensuring it was in compliance with both the letter and spirit of the law. I am appending to my testimony a memorandum discussing in greater detail NebuAd's compliance with the law, including the cable privacy statute over which this Subcommittee has jurisdiction.

The NebuAd service is architected and its operations are based on principles essential to strong privacy protection:

- Provide users with prior, robust notice and the opportunity to express informed choice about whether to participate, both before the service takes effect and persistently thereafter;
- Do not collect or use personally-identifiable information ("PII");[1]
- Do not store raw data linked to identifiable individuals; and
- Provide state-of-the art security for any information stored.

As a result, NebuAd's service is designed so that no one – not even the government – can determine the identity of our users. That means our service for ISP users, including the ad optimization and serving system, does not collect or use any PII. In addition, NebuAd requires its ISP partners to provide robust, advance notice about our operations and our privacy protections to their subscribers, who at any time can exercise their choice not to participate. And, finally, we have located our servers in highly secure data centers.

THE NEBUAD TECHNOLOGY AND ITS ADVERTISING OPERATIONS

Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual web-sites to networks of web-sites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an

[1] NebuAd does not collect or use personally identifiable information about Internet consumers, and it ensures the anonymous information that its systems infer cannot be used to identify any individual. None of the anonymous information NebuAd stores can be compiled together and somehow reverse engineered to identify any individual. In other words, the information is not "pseudo-anonymous." NebuAd is able to ensure this critical privacy protection by building many safeguards into its system including: completely anonymous user profiles which only store levels of qualifications for market segment categories; market segment categories that are kept sufficiently broad and aged sufficiently rapidly; no connection or link between the ISP's registration data systems and NebuAd; and, no collection of information from any small, identifiable group (such as by specific 9-digit zip-code information).

Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the ads shown. And when a user visits a web-site within an online advertising network, some of which include thousands of sites, the visits help the network advertising company categorize a user for targeted advertising. All of these activities are well-entrenched in the Internet and, given the enormous and growing use of the Internet, have proven to have mutual benefits for users, publishers – large and small – advertisers, and ad-networks.

NebuAd provides online advertising in partnership with ISPs. The NebuAd advertising service – part of which is collocated with, but operates separate and apart from, an ISP's facilities – has been architected to use only a select set of a user's Internet activities (that is, only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user. The NebuAd advertising service does not collect or use any information from password-protected sites (*e.g.*, HTTPS traffic), web mail, email, instant messages, or VOIP traffic. Using only non-PII, NebuAd constructs and continuously updates these unique and anonymous user profiles.[2]

In the course of these business operations, NebuAd's ad optimization and serving system does not collect PII or use information deemed to be sensitive (*e.g.,* information involving a user's financial, sensitive health, or medical matters). In addition, NebuAd requires its ISP partners to provide robust disclosure notices to users prior to initiating any service and permits them to opt-out of having their data collected and receiving targeted ads. Once a user opts-out,

[2] The anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent the anonymous inferences about the user's level of qualification for a predefined set of market segment categories.

NebuAd deletes that user's anonymous user profile and will ignore the user's subsequent web navigation activity.[3]

Finally, NebuAd's ad optimization and serving system operates similar to traditional ad networks. It makes standard use of cookies for accepted ad serving purposes. It makes standard use of pixel tags that operate only within the security framework of the browser to invoke the placement of ad network cookies and that contain no uniquely identifying number, subscriber identifier, or any other subscriber information. In sum, NebuAd's code used for standard ad serving purposes is both clean in its purpose and function.

THE PRIVACY PARADIGM IN THE UNITED STATES AND NEBUAD'S PRIVACY PROTECTIONS

In contrast to the European Community, where omnibus privacy law covers all industries, in the United States, privacy statutes have been developed in a largely sector-specific fashion. This Subcommittee and the larger Energy and Commerce Committee have long been part of that trend, having overseen the creation of privacy statutes generally covering the cable and telecommunications industries, as well as specific statutes addressing online privacy for children, telemarketing, and spam. Yet, even though these and other privacy statutes have been developed one at a time, there are common threads running through them:

- When more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed.

- When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

[3] NebuAd has enhanced the industry-standard opt-out "cookie" based system with the use of proprietary techniques. This enables the opt-out to be more persistent. NebuAd's entire enhanced opt-out system is linked to individual computers and browsers, and it informs users of this fact in assisting them in understanding the nature of their opt-out choice.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business-neutrality.

In implementing this privacy paradigm, NebuAd not only relied on the expertise of its own personnel, it turned to leading privacy experts, including Fran Maier, Executive Director and President of TRUSTe, the consumer privacy organization, Dr. Larry Ponemon of the Ponemon Institute, and Alan Chapell of Chapell & Associates. These experts provided important input into NebuAd's initial privacy program. They were particularly stringent in recommending that NebuAd should not collect PII or sensitive information and that it provide consumers with robust notice and choice. NebuAd followed that guidance in developing our privacy program.[4]

The following summarizes the key privacy protections upon which NebuAd has architected into its technology and based its operations and which ensure its activities and that of its ISP partners are in compliance with federal and state laws:

> **1. NebuAd's service does not collect or use PII from ISP subscribers.** The entire ad optimization and serving system does not collect or use any PII, nor does it collect any information from password-protected sites, web mail, e-mail, instant messages, or VOIP traffic.
>
> **2. NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles").** NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual. Rather, the NebuAd service constructs

[4] A just released survey of U.S. Internet users by TRUSTe showed that 71% of online consumers are aware their web-surfing information may be collected for the purpose of advertising and 91% wanted to have the tools to assure they could protect their privacy. NebuAd has strived to provide users with this transparency by educating users about its activities and their choices regarding whether to participate in NebuAd's services.

anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. NebuAd's ISP Partners are required to provide robust, direct notice in advance of launch of the service. The notice discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web-surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service. For existing subscribers, the notice is required to be delivered 30-days prior to the launch of the service by postal mail, e-mail, or both.[5] For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and on-going disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service. Users are provided with a clear statement of what opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.[6]

5. NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous. NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one – not even NebuAd's engineers who designed the system – can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

6. NebuAd avoids any sensitive websites or product categories. NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII. This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the consumer's level of qualification for a predefined set of market segment categories. Raw data is simply not

---

5 NebuAd seeks to ensure that users are fully informed of its activities and are given full opportunity to choose whether to participate. To that end, we are developing enhanced notification mechanisms.

6 The user, of course, will continue to receive ads.

stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. There is no connection or link between the ISP's registration data systems and NebuAd. That means that no user-specific data is exchanged between NebuAd and ISP data systems. This boundary is preserved further and inadvertent disclosure is prevented because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. NebuAd installs no applications on users' computers, has no access to users' hard drives, and has no access to secure transactions. As such, NebuAd does not control a user's computer or web-surfing activity in any way (*e.g.,* by changing computer settings or observing private or sensitive information).

10. NebuAd's Data Centers are professionally operated and secured. NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

NebuAd is proud of these protections – all of which were adopted to comply with both the spirit and letter of the government's privacy paradigm – and, it continuously seeks to enhance them.

CONCLUSION

As I stated at the outset, I have spent years seeking to ensure that users have robust and transparent privacy protections. In a very real sense, NebuAd is the product of that work. It has adopted and implemented state-of-the-art privacy protections, and, equally as important, it has established a process to continuously improve on them. The Internet is a highly dynamic environment, where new technologies are constantly developed to address new challenges, and we both want and need to take advantage of them. NebuAd and its ISP partners take their responsibilities to Internet users very seriously. NebuAd looks forward to continuing to work with government policymakers as they examine online advertising and privacy issues.

MEMORANDUM

JULY 17, 2008

FROM: NEBUAD, INC.

RE: LEGAL AND POLICY ISSUES SUPPORTING NEBUAD'S SERVICES

I. Introduction to NebuAd

NebuAd is an online media company founded by Internet security experts in 2006. It provides online advertising in partnership with ISPs, using a select set of a user's Internet activities (only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification with respect to a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user.

NebuAd is a newcomer to the world of online advertising. This world of Internet companies includes several industry giants, behavioral advertising networks, and countless website publishers. Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual websites to networks of websites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the sponsored search results and ads shown. When a user visits websites within an online advertising network, some of which include thousands of sites, the visits help the advertising network track the user for the purpose of serving higher-value targeted advertising. All of these activities are well-entrenched in the Internet and have become fundamental to the economic model that underpins the wide availability of content and services on the Internet today. These advertising capabilities, have proven to have mutual benefits for users, publishers – both large and small – and advertisers.

NebuAd offers a unique business model that allows ISPs to participate in the online advertising ecosystem, while not only adhering to industry-standard privacy policies but also establishing new state-of-the-art privacy protections and user choice policies that go far and beyond those used on the Internet today.

Given the background of its founders, NebuAd architected its service and its policies to adhere to very strict privacy principles. These include:

1. NebuAd's service does not collect or use PII from ISP subscribers. The entire ad optimization and serving system does not collect or use any Personally Identifiable Information (PII), nor does it collect any information from password-protected sites, web mail, email, instant messages, or VOIP traffic.

2. NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles"). NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual.

Rather, the NebuAd service constructs anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. NebuAd's ISP Partners are required to provide notice to users in advance of launch of the service. The notice, which must be direct and robust, discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service. For existing subscribers, the notice is required to be delivered 30 days prior to the launch of the service by postal mail, email, or both. For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and on-going disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service. Users are provided with a clear statement of what the opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.'

5. NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous. NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one – not even NebuAd's engineers who designed the system – can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

6. NebuAd avoids any sensitive websites or product categories. NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII. This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the user's level of qualification for a predefined set of market segment categories. Raw data is simply not stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. There is no connection or link between the ISP's registration data systems and NebuAd. That means that no user-specific data is exchanged between NebuAd and ISP data systems. This

---

The user, of course, will continue to receive ads.

boundary is preserved further, and inadvertent disclosure is prevented, because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. NebuAd installs no applications of any type on users' computers, has no access to users' hard drives, and has no access to secure transactions. As such, NebuAd does not control a user's computer or web-surfing activity in any way, e.g., by changing computer settings or observing private or sensitive information.

10. NebuAd's Data Centers are professionally operated and secured. NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

II. The Federal Wiretap Act

As a threshold matter, it is important to note that the federal Wiretap Act[2] was last amended in 1986 before the widespread adoption of personal computing and online communications.[3] When the Wiretap Act was enacted, and amended, the focus was on telephone communication and other similar technology. Case law is rich with examples of claims involving a tapped phone line.[4] Notably, these cases primarily involve direct, one-on-one communication between the parties. The content is personal to the speakers, such that if one of the parties was replaced, the communication would not contain the same content. Although secrecy or confidentiality was not expressly built into the Wiretap Act, the Act was enacted at a time when the focus was on individual communications—likely as a result of the limitations of then-existing technology.

The environment that has since evolved for online communications is markedly different. While online communications are still carried by *wire,* there are important policy distinctions between the types of communications that the Wiretap Act was enacted to address, and the types of communications present in the online environment today. Internet users are not engaged in a personal, direct conversation with non-secure website publishers.[5] Such publishers provide online content indiscriminately to all users. As stated below, even under the Wiretap Act, courts look to the circumstances surrounding a communication.[6] Yet, the evaluation of circumstances

---

[2] 18 U.S.C. §§ 2510-2522.

[3] The Wiretap Act was amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986). While the Wiretap Act is Title I of the ECPA, it was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III."

[4] *See, e.g., United States v. Foster,* 580 F.2d 388 (10th Cir. 1978) (telephone company taps phone line of user suspected of defrauding the telephone company out of long-distance charges); *United States v. Harvey,* 540 F.2d 1345 (8th Cir. 1976) (same); *United States v. Auler,* 539 F.2d 642 (7th Cir. 1976) (same).

[5] There are always exceptions to this statement, such as online purchases, encrypted communication, and other secured data transactions, but notably, these private communications are the exact types of information that NebuAd's services do not collect. NebuAd's services personalize generic content rather than intruding upon private communications.

[6] *See United States v. Amen,* 831 F.2d 373, 378 (2d Cir. 1987).

that surround a telephone communication between two parties is not analogous to an online communication between a party and a website. To date, there are no litigated decisions directly addressing the application of the Wiretap Act to a URL provided as part of a consumer's online navigations or provided via publicly available search request and response. Therefore, it is still an open question as to whether these types of communications are even covered by the Wiretap Act.'

Assuming, for the purposes of this memorandum, that the Wiretap Act applies to NebuAd's services, the Act expressly prohibits the intentional interception of an electronic communication[8] unless "one of the parties to the communication has given prior consent to such interception."[9] The legislative history of the Wiretap Act clearly indicates "that Congress intended the consent requirement to be construed broadly."[1o] As a result, "courts have resoundingly recognized the doctrine of implied consent."[11] The Court of Appeals for the Second Circuit stated that the Wiretap Act "affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent."[12]

To determine whether a party has impliedly consented to an interception under the Wiretap Act, courts examine the totality of the circumstances and "imply consent in fact from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance."[13] In such evaluations, courts have found that parties impliedly consented to an interception in various fact patterns. The federal district court for the Southern District of New York found implied consent when an employer circulated memoranda regarding telephone monitoring and recording.

---

[7] *See* Patricia L. Bellia, *Spyware: The Latest Cyber-Regulatory Challenge,* 20 BERKELEY TECH. L.J. 1283, 1296, 1311-12 (2005). Another law review article described the question as to whether URLs contain contents as "surprisingly difficult" and "quite murky." Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 Nw. U. L. REV. 607, 645-46 (2003).

[8] 18 U.S.C. § 2511(1)(a).

[9] *Id. §* 2511(2)(d).

[1o] *United States v. Amen,* 831 F.2d 373, 378 (2d Cir. 1987) ("Consent may be expressed or implied. Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to.'" (quoting S. Rep. No. 1097, 90th Cong. 2d Sess., *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182)).

[11] *George v. Carusone,* 849 F. Supp. 159, 164 (D. Corm. 1994); *see United States v. Faulkner,* 439 F.3d 1221, 1224-25 (10th Cir. 2006) ("We are not persuaded to depart from the unanimous view of the *holdings* by our fellow circuit courts."); *United States v. Corona-Chavez,* 328 F.3d 974, 978-79 (8th Cir. 2003); *Griggs-Ryan v. Smith,* 904 F.2d 112, 118 (1st Cir. 1990); *United States v. Willoughby,* 860 F.2d 15, 19-20 (2d Cir. 1988); *Amen,* 831 F.2d at 378; *United States v. Tzakis,* 736 F.2d 867, 870, 872 (2d Cir. 1984); *Borninski v. Williamson,* No. Civ. A. 3:02CV1014-L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005); *United States v. Rittweger,* 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003); *Chance v. Avenue A, Inc.,* 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litig.,* 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).

[12] *Griggs-Ryan,* 904 F.2d at 116.

[13] *Amen,* 831 F.2d at 378.

Although the party denied receiving the notice, and evidence proving such receipt was destroyed, the court determined that the party had knowledge of the monitoring and recording and impliedly consented to such monitoring and recording by continuing to use the monitored telephone lines.[14]

Similarly, a Connecticut federal district court found that employees had given their implied consent to the recording of conversations on work telephones, as many of the telephones displayed warning labels, memoranda were circulated to all employees regarding the recording of incoming and outgoing telephone calls.[15] The court stated that employees' "knowledge of the system and subsequent use of the phones is tantamount to implied consent to the interception of their conversations."[16] The Court of Appeals for the First Circuit held that repeated oral statements that all incoming telephone calls would be monitored was sufficient notice, and that the party's taking an incoming phone call was implied consent to the interception." Additionally, a Texas federal district court found that an employee consented to monitoring of Internet communications at work because the employee had signed a form stating that "Internet access should be limited to 'business use only,' and that the company 'logs and archives all incoming and outgoing data communications through its gateway system. Use of the gateway implies consent to such monitoring.'"[18]

Using the framework established by the courts, NebuAd satisfies the implied consent exception to liability for interception under the federal Wiretap Act.[19] NebuAd requires, by contract, that all of its ISP partners give subscribers notice of NebuAd's services, including the collection of anonymous information regarding subscribers' online activities, for use in advertising. This notice must be given directly, and prior to the initiation of the ISP's use of NebuAd's services. The ISP partners are also required, by contract, to alter their privacy policies accordingly. NebuAd further requires that all ISP partners provide users with an option to opt-out of NebuAd's services, initially upon receipt of the direct notice, and in an ongoing manner through the ISP's privacy policy.

---

[14] *Rittweger,* 258 F. Supp. 2d at 354.

[15] *George,* 849 F. Supp. at 164.

[16] *Id.*

[17] *Griggs-Ryan,* 904 F.2d at 117-19.

[18] *Borninski v. Williamson,* No. Civ. A. 3:02CV1014-L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005).

[19] Website publishers may also consent to an interception, as website publishers make web content available for any user. Such posting does not constitute an exclusive communication between the website publisher and the user, but rather it is public communication that is intended to be viewed by any number of simultaneous users. As a result, website publishers have no reasonable expectation that the communication between it and any consumer will remain private or confidential, and thus impliedly consent to the interception by a third party.

III. The Cable Act

The Cable Act[20] was enacted to protect cable subscribers' personal information. Among other things, it requires cable operators to obtain written or electronic consent from a subscriber prior to collecting any PII concerning the subscriber.[21] In addition to the limitations on the collection of subscriber PII, the Cable Act limits the disclosure of subscriber PII by cable operators.[22] The Cable Act sets out multiple standards that a cable operator must satisfy in order to disclose subscriber PII. If the disclosure is necessary for a legitimate business activity, a cable operator is not required to provide the subscriber with any notice.[23] A cable operator may disclose the name and mailing addresses of subscribers if it provides subscribers with the opportunity to opt out of such disclosure.[24] For all other disclosures of subscriber PII, a cable operator must obtain "the prior written or electronic consent of the subscriber"—essentially an opt-in standard.[25]

Notably, under the Cable Act, PII "does not include any record of aggregate data which does not identify particular persons."[26] The Cable Act does not define PII beyond this exclusion. The legislative history expressly states:

> The phrase 'to collect personally identifiable information' covers the various ways that individuals can be identified, including name, address, and social security number. It is not intended to cover the electronic collection process used to produce aggregate records that are not individually identifiable. Such aggregate records indicate how groups of subscribers—such as males or residents of a certain neighborhood—use the system, and therefore pose no perceivable privacy threat to individuals.[27]

Courts have used this legislative history as the foundation to further define the limits of PII under the Cable Act, and the limited number of litigated decisions yield findings consistent with the legislative history and the traditional definitions of PII, such as "specific information about the subscriber, or a list of names and addresses on which the subscriber is included, but does not include aggregate information about subscribers which does not identify particular persons."[28]

---

[20] Cable Communications Policy Act (1984), 47 U.S.C. §§ 551-561.

[21] *Id. §* 551(b)(1).

[22] *Id. §* 551(c).

[23] *Id. §* 551(c)(2)(A).

[24] *Id. §* 551(c)(2)(C)(i).

[25] /d. § 551(c)(1).

[26] *Id. §* 551(a)(2)(A).

[27] S. REP. No. 98-67, 98th Cong., 1st Sess. 28 (1983).

[28] H.R. REP. No. 934, 98th Cong., 2d Sess. 79 (1984); *see, e.g., Pruitt v. Comcast Cable Holdings, LLC,* 100 F. App'x 713, 2004 WL 1226937, at **2 (10th Cir. 2004) (quoting same language from H.R. REP. No. 934); *Scofield v. Telecable of Overland Park, Inc.,* 973 F.2d 874, 876 (10th Cir. 1992) (same); *Parker v. Time Warner Entm't Co.,* No. 98 CV 4265(ERK), 1999 WL 1132463 (E.D.N.Y. Nov. 8, 1999) (stating that collection of subscriber race, ethnicity, age, income, dwelling type, and telephone number packaged along with individual subscriber name

In *Pruitt v. Cox Cable Communications,* a 2004 case before the Court of Appeals for the Tenth Circuit, the court examined the application of the Cable Act to subscriber data stored in a converter box, which contained a "unit address" that can be matched to a billing system. The court found:

> [T]he converter box code—without more—provides nothing but a series of numbers. . . . Without the information in the billing or management system one cannot connect the unit address with a specific customer; without the billing information, even [the cable operator] would be unable to identify which individual household was associated with the raw data in the converter box. Consequently, it is the billing system that hold the key to obtaining personally identifiable information, not the converter box.[29]

Similar to the court's finding in *Pruitt,* NebuAd's service specifically complies with the Cable Act because NebuAd's service does not collect PII. Instead, using only non-personally identifiable information, NebuAd uses a select set of a user's Internet activities (a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories, which are then used to select and serve the most relevant advertisements to that user. The use of NebuAd's services certainly does not require a subscriber to opt-in—the strictest notice and consent requirement. Although not an activity conducted by NebuAd, even the disclosure of a subscriber's mailing address, widely recognized as PII, only requires that the subscriber have an opportunity to opt-out. NebuAd's service, on the other hand, does not even collect subscriber PII. Because NebuAd's service does not collect subscriber PII, there is no violation of the Cable Act.

Additionally, a 2002 FCC ruling concluded that "cable modem service, as it is currently offered, is properly classified as an interstate information service, not as a cable service, and that there is no separate offering of a telecommunications service."[30] This determination that cable interne

---

services are not classified as telecommunications services was upheld by the Supreme Court as a

and address is PII); *Nat'l Satellite Sports, Inc. v. Eliadis, Inc.,* No. 5:97CV3096, 1998 WL 695246, at *5 (N.D.Ohio Sept. 10, 1998) (holding that list identifying residential cable subscribers is PII); *United States v. Cox Cable Commc'ns,* No. 98CV118/RV, 1998 WL 656574, at *1 (N.D.Fla. Apr. 28, 1998) (quoting same language from H.R. REP. No. 934, and stating that a customer's cable billing and payment history is PII) *Metrovision of Livonia, Inc. v. Wood,* 864 F. Supp. 675, 681 (E.D. Mich. 1994) (records from a fraud detecting device used by a cable provider are not PII). Several cases also cite the legislative history referencing general privacy interests, and the capability of cable systems to collect information such as bank transactions, viewing habits, and significant personal decisions using subscriber records from the interactive cable systems. Such information may be PII if it is specifically linked to and can be used to identify individual subscribers, but not if it is information contained in an anonymous user profile. While these types of information may be general privacy considerations, of which Congress was expressly aware, Congress chose to enact the definition of PII such that it "does not include any record of aggregate data which does not identify particular persons." 47 U.S.C. § 551(a)(2)(A).

[29] *Pruitt,* 100 F. App'x 713, 2004 WL 1226937, at **3.

[30] *In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities,* 17 FCCR 4798, 4802 (2002).

lawful interpretation of the Communications Act.[31] A recent decision by the Court of Appeals for the Sixth Circuit upheld this distinction and stated that the plain language of the Cable Act precludes its application to broadband internet services, even those provided by a cable operator.[32] Examining the application of the Cable Act, the court emphasized that as the cable provider was providing broadband internet access and not cable service, the Cable Act was inapplicable.[33]

IV. Policy Implications

NebuAd provides users with a great amount of privacy protection. Unlike many online advertising models today, NebuAd's service does not collect or use any PII. In addition, NebuAd's anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent anonymous inferences about the user's level of qualification for a predefined set of market segment categories. (NebuAd does retain some anonymous data for analysis and reporting.) Additionally, NebuAd is one of the only models—if not the only model—that provides users with advance notice of the nature of its services and an opportunity to opt-out *before* the service takes effect. NebuAd's service also complies with the government's consent policy on privacy as NebuAd's service does not collect any PII, and provides users with the opportunity to opt-out.[34] Finally, NebuAd's service does not observe encrypted traffic, does not observe VOIP sessions, does not store raw search queries linked to an identifiable user, and does not track users' IP addresses, thus providing an excellent set of privacy protections. Because of the privacy protections that NebuAd has incorporated into the architecture of its service, it is able to provide users with relevant advertising messages in a safe, secure, and privacy-respecting manner.

---

[31] *Nat'l Cable and Telecomms. Ass 'n v. Brand X Internet Servs.,* 545 U.S. 967 (2005).

[32] *Klimas v. Comcast Cable Commc'ns, Inc.,* 465 F.3d 271 (6th Cir. 2007), *reh'g en banc denied Klimas v. Comcast Cable Commc'ns, Inc.,* 2007 U.S. App. LEXIS 13658 (6th Cir. May 1, 2007).

[33] A few courts have applied the disclosure provisions of the Cable Act to broadband internet services in the limited context of discovery proceedings under the Federal Rules of Civil Procedure. *See, e.g., Warner Bros. Record Inc. v. Does,* No. 07-706 (RJL), 2008 WL 60297 (D.D.C. Jan. 4, 2008); *Arista Records LLC v. John Does 1-19,* 245 F.R.D. 28 (D.D.C. 2007). *But see, Interscope Records v. Does 1-7,* 494 F. Supp. 2d 388, 390 (E.D. Va. 2007) (stating that "only a government entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order," and denying an *ex parte* subpoena under the Cable Act) (internal quotation omitted). In these cases, the courts compelled ISPs to release PII of otherwise unidentifiable defendants to plaintiffs in the course of litigation unrelated to the ISPs activity. Such disclosure occurred only after the plaintiffs exhausted their ability to identify the defendants, thus requiring information from the ISPs for the suits to progress any further. *Warner Bros.,* 2008 WL 60297, at *1; *Arista Records,* 246 F.R.D. at 28-29. These cases did not recognize a right of action against the providers of broadband internet service under the Cable Act.

[34] Use of a consumer opt out is consistent with other consumer information protection statutes such as the Gramm-Leach-Bliley Act (financial Data), the Health Insurance Portability And Accountability Act (health data), the Fair Credit Reporting Act (consumer reports), the

Telemarketing and Consumer Fraud and Abuse Prevention Act (telemarketing), and the CAN-SPAM Act (email marketing)